CAMDEN COUNTY DEVELOPMENTAL DISABILITY RESOURCES

TECHNOLOGY PLAN

(Revised October 20th, 2014)

This Technology Plan provides an overview of Camden County Developmental Disability Resources (CCDDR) information technology (IT) systems, security, confidentiality, and disaster recovery. CCDDR utilizes IT for a variety of reasons, including:

- To allow staff to adequately do their jobs
- To provide for informed decision-making both with regard to administrative as well as programmatic functions based upon analysis of available data
- To provide those served with quality services and supports

The following information summarizes CCDDR's Information Technology system, compliance with current regulations and guidelines, and action plan needed to enhance or improve CCDDR's current IT system and/or required for compliance issues. All IT needs identified in this plan shall be incorporated as budget items and/or otherwise approved by the Board of Directors in CCDDR's current year budget or proposed budget for future fiscal years.

Agency Hardware/Software Systems

The status of CCDDR hardware and system software plays a vital role in allowing staff to properly complete their work. Systems in place must meet industry standards as well as standards specific to the work to be accomplished at CCDDR. In addition, computer systems play a role in assuring that all computer users have the capabilities to follow through on security and confidentiality procedures, as well as continual operation in case of theft or disaster.

Hardware

CCDDR currently has desktop systems in place for each employee as well as servers for each office location; tablet or laptop computers for each Support Coordinator and administrative staff; printers for each workstation; routers for the Targeted Case Management (TCM) and Administrative offices; "hub's" for each office network; and all related accessories for each system. All CCDDR computer systems are periodically updated to allow for compatibility with the most recent software programs for compliance with our current technology plan. Any desktop computer system or device not meeting with current system minimal requirements may not be installed to the CCDDR network system.

Software

All networks, systems, and servers now have the most recent versions of the Windows operating systems, most recent security software available in the market, and the most recent firewalls available in the market. Main software programs installed on all desktop systems include Microsoft Office, Adobe Acrobat, security software, Windows Media Player, and other ancillary programs. All desktop systems are linked via a network server. All hardware is less than 5 years-old. Operating system software, office software, network software, and other office programs are up-to-date and meet current industry standards, which allow for the latest in security settings and encryption to be installed to the network and internet. Any system that does not meet the minimal software requirements may not be installed to the network/internet.

Inventory

Inventory of all systems, with their current operating capacities, date of activation and current authorized users are updated on a regular basis by the Compliance Manager and IT Administrator. Any computer not included in the list of inventory, and thus inspected, may not be installed to the network/internet.

Security/Confidentiality

Security and Confidentiality practices are the most important aspect of any organization working with sensitive, confidential information. CCDDR's current practices allow for complete protection of sensitive information from unauthorized outside and inside intrusion, as well as proper procedures for handling sensitive and private information electronically through such mediums as e-mail, network or, internet.

Password Security

All users have individual usernames and passwords that comply with industry standards and eliminate unauthorized access. All passwords must meet the following requirements:

- Not a word in the dictionary
- Are 9 or more characters in length
- Include a case sensitive character
- Include a number or character

Separate passwords are to be used for logging on to the logging/billing systems.

Keeping or making hard copies of usernames and passwords for an extended period of time is prohibited. Employees are instructed to devote them solely to memory and not share them with unauthorized personnel. Passwords for both

the CCDDR network and the logging/billing systems shall be changed on a periodic basis. Temporary copies for general use should be destroyed after devoted to memory or the task completed. Passwords are not to be shared with other CCDDR staff, family members of staff, etc.

File & Network Security

CCDDR promotes flexibility and efficiency for staff to complete job assignments and meet the needs of the consumers served; however, to prevent unauthorized access to confidential information and to protect the integrity of the data, the following must be adhered:

- All digital information, folders, and files are organized by staff and personal files/folders are only accessible by authorized users
- All files that need to be protected and are confidential must be stored on the network drives or temporarily stored on remote access devices issued to staff (tablets and laptops)
- Only the Executive Director, contracted IT personnel, or other staff authorized by the Executive Director have the proper security rights to administer the network
- The network can only be accessed remotely by tablet or laptop computers issued to the staff by CCDDR through secured software set up by IT personnel
- Employees working remotely should save files to the tablet or laptop computer issued to them, transfer and save data to the CCDDR network the next day in the office, or transfer data via the secured software to the CCDDR network – personal staff computers should never be used and no client information should be saved to the employee's home computer system
- No confidential information should be saved to an external drive or disk – information not confidential can be saved to external drives or disks, but must be also be saved or backed-up to a CCDDR tablet, laptop, or computer workstation
- Confidential files submitted as attachments over the internet, names within the context of electronic transmissions, or other confidential information must be encrypted through secured software procured by CCDDR or the State encryption email system

Individual Firewalls

In addition to a Network firewall, individual desktop, laptop, and tablet firewalls are used as a redundant precaution.

Staff Requirements for Use of Web-Based Logging/Billing Systems Remotely

The logging/billing systems are web based systems designed for user convenience and can be accessed from other computers via the Internet. Nevertheless, security and confidentiality of consumer information needs to be maintained. The following guidelines apply to all CCDDR employees when accessing these systems remotely:

- As a general rule, staff should only access these systems from their assigned CCDDR tablet or laptop computer and not in the presence of others – access from a public place is prohibited.
- No other members of employee's family are authorized to view confidential information, so steps should be taken for use in secure locations.
- Due to security concerns, only secured wireless connections can be used to access these systems remotely
- Passwords for accessing these systems are not to be written on paper in employee's home or other remote location, but rather committed to memory.
- Networks being used to work remotely must have the same security features as the CCDDR network systems

Counter Intrusion & Virus protection

Measures to control unwanted intrusions from outside attacks, such as viruses and hackers, are a real threat; however, with simple preventive technologies, such as firewalls and virus protection software, and with proper training, this type of threat can be controlled and eliminated.

Counter Intrusion

To prevent unauthorized access to confidential information and to protect the integrity of CCDDR's data, the following must be adhered:

- Firewall and Broadband Modem Firewall Routers are to be maintained and updated as necessary
- Routers should be replaced if they become obsolete, damaged, or can no longer provide the proper security settings to meet the current and future protection for use on the internet 24 hours a day
- The server should maintain a firewall connection to the Internet
- Connection to the internet on the server should be enabled only to perform updates or other such temporary tasks as an added security measure

Virus Protection

A managed virus/internet security application will be maintained at all times. Updates, scanning, and other functions are to be managed using network virus protection utilities to ensure real time administration of virus program activities and scanning results.

The most recent and best software in the market has been employed within all CCDDR desktop, laptop, tablet, and network systems. In addition to daily scanning and individual file scanning, the current security software has the following capabilities:

- Automatic daily updates of new circulating viruses
- Complete e-mail scanning and certification
- Network management capabilities
- Low system resource usage
- Can be managed remotely
- Contains spyware/malware detection

Theft and Disaster Recovery

Theft and disasters, such as fire, flood, and natural disasters, are unpredictable and can often result in complete destruction of a company's digital information. However with proper preventive measures, these threats can be managed and data can be recovered in a timely manner. To prevent the loss of data and digital information, the following must be adhered:

- Complete backups of work related data that are stored on all CCDDR network folders are to be backed up on a nightly basis locally and weekly basis remotely (Web-based or other similar method) – backups are to be stored in high performance removable hard drives and reliable, secure remote locations that can hold and retrieve information quickly and reliably.
- Only the authorized system administrator or Executive Director can retrieve password protected data from the backup hard drive
- In addition to daily backups, secondary backups are performed on each tablet, laptop, and work station to ensure quick recovery of data and increase the chances of retrieving lost or misplaced data

Disaster Recovery

All systems attached to the network can be replaced and restored to their original state after replacement of the hardware due to volume licensing and current backup procedures. Volume licensing allows software property to be defined by codes and serial numbers, which are digitally stored and cannot be lost. Once the new hardware is replaced, the software can be reinstalled using current

operational licenses or OEM system software that came with the system. The file server that stores all of the data can also be replaced as described above.

A stolen system is useless without the proper passwords; however, the hard drive is vulnerable to hacking. Saving all confidential or vital company data on the network drives will make them unavailable in a stolen computer stolen.

Staff Training

For any technology plan to be fully effective employees must understand and be trained to follow proper network user protocols. Efforts must be made to continuously offer training and courses to keep CCDDR network users up to date and informed about the network and network regulations. The following are a few of the concepts and tasks all users should know and be trained to perform:

- Network
- Local drive vs. network drive
- Folder vs. file
- Saving documents to network drives
- Understand network security
- User name/password & user permission
- Shared folders
- Network groups vs. single users
- Administrator vs. standard user
- Software and hardware
- E-mail security etiquette & concepts
- E-mail virus scanning
- Types of e-mail viruses and how they spread
- E-mail attachments
- Spyware and adware awareness
- Using links delivered through e-mail and the dangers involved
- Fishing and e-mail scams
- Virus protection
- Reporting errors
- Virus and worm types
- E-mail vs. browser viruses

Staff training on these subjects is to be provided by an IT professional or the Executive Director periodically.

Accessibility

CCDDR needs to have technology that is accessible to both staff and persons served. Technology in the work place can either create barriers to persons with various types of disabilities, or, alternatively, be a liberating force for persons with

disabilities. This is true not only in terms of hardware and software utilized by CCDDR employees, but also with regard to the CCDDR Web site and other media sites.

Assistive/accessible technology products are specialty products designed to provide additional accessibility to individuals who have physical or cognitive difficulties, impairments, and disabilities. When selecting assistive technology products, it is critical to find products that are compatible with the computer operating system and programs on the particular computer.

Some of the ways that employees should be able to customize their computer system include:

- Change font size, color, and type of text on screen
- Adjust text and background colors
- Adjust sound options including the ability to get audio information visually (such as closed captioning or audio descriptions for multi-media) as well as aurally
- Adjust timings
- Eliminate or modify the rate of flashing or blinking
- Get alternatives for touch screen applications
- Customize toolbars for easy access to buttons used most often
- Adjust keyboard settings to compensate for impairments such as hand tremors, or people who use select fingers, one hand, or no hands
- Operate a computer with a keyboard instead of a mouse
- Increase the visibility of the cursor
- Add assistive technology products for specific disabilities
- Use an alternative kind of mouse because of mobility impairments

In addition, CCDDR's technology ideally should provide ways for employees to:

- Easily access Web sites
- Use e-mail to collaborate and communicate
- Use a word processing system to collaborate
- Share documents
- Manage large amounts of data
- Sort and manage files and folders

Internet Services

Having a Web site and other media sites for the agency allows for better outreach services to be conducted by CCDDR and would spread the word about our agency and what we do to assist persons with developmental disabilities. CCDDR will either employ third-party professionals or appoint an employee to maintain and update its Web site and media sites to ensure ease of access, continual reference for pertinent information, news of changes, announcements, etc.

IT Support Services

CCDDR utilizes the services of an IT consultant who is under contract with the board. The consultant is responsible for network administration and problem-solving/repair on an as-needed basis. CCDDR also utilizes IT support/consultant services with regard to the logging/billing internet-based case management systems. CCDDR has access to the Department of Mental Health “CIMOR” database, which is managed by the Department of Mental Health.